FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards
and Technology of the United States
of America

The Communications Security
Establishment of the Government
of Canada

Consolidated Certificate No. 0037

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Michael J Cooper
Dated: 2/12/2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:
Dated: 6 Feb 2014

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2070	01/24/2014	Common Crypto Module for PRIISMS, PRIISMS RD, SA5600-IA and NetGard MFD	API Technologies Corp.	Software Version: 1.0
2071	01/24/2014	ETERNUS DX400/DX8000 Controller Module	Fujitsu limited	Firmware Version: V20L80-1000
2072	01/29/2014	HiCOS PKI Native Smart Card Cryptographic Module	Chunghwa Telecom Co., Ltd.	Hardware Version: RS45C; Firmware Version: HardMask: 2.2 and SoftMask: 1.0
2073	01/29/2014	GoldKey Security Token Cryptographic Module	GoldKey Security Corporation	Hardware Version: IC USB-CONTROLLER-2LF; Firmware Version: 7.12
2075	01/29/2014	Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with Wireless Services Modules-2 (WiSM2)	Cisco Systems, Inc.	Hardware Versions: Chassis: Catalyst 6506 switch [1], Catalyst 6506-E switch [2], Catalyst 6509 switch [3] and Catalyst 6509-E switch [4]; Backplane: WS-C6506 [1], WS-C6506-E [2], WS-C6509 [3] and WS-C6509-E [4]; FIPS Kit: P/N 800-27009 [1, 2], P/N 800-26335 [3, 4] and WS-SVCWISM2FIPKIT= [1, 2, 3, 4]; with one Supervisor Blade [1, 2, 3, 4]: [WS-SUP720-3BXL, WS-SUP720-3B, VS-S720-10G-3C or VS-S720-10G-3CXL] and with one WiSM2 [1, 2, 3, 4]: [WS-SVC-WISM2-K9=, WS-SVC-WISM2-5-K9=, WS-SVC-WISM2-3-K9=, WS-SVC-WISM2-1-K9=, WS-SVC-WISM2-5-K9, WS-SVC-WISM2-3-K9 or WS-SVC-WISM2-1-K9]; Firmware Version: Supervisor Blade: Cisco IOS Release 12.2.33SXJ, Cisco IOS Release 12.2.33SXJ1 or Cisco IOS Release 12.2.33SXJ2; WiSM2: 7.0.240.0